This is Information Retrieval

If we're going to have an ID card, let's have a 21st century ID card

David G.W. Birch
Director
Consult Hyperion
8 Frederick Sanger Road
Guildford
Surrey GU2 7ED

Telephone +44 (0)1483 301793
Fax +44 (0)1483 561657
E–mail dave.birch@chyp.com
Web http://www.chyp.com/

David G.W. Birch is a Director of Consult Hyperion—the IT management consultancy that specialises in electronic transactions—which he helped found after several years working as a consultant in Europe, the Far East and North America. A physicist by training, Dave has lectured on the impact of new communications technologies to MBA level. He is European correspondent for the *Journal of Internet Banking and Commerce*, a member of the editorial advisory the *European Business Review* and is a European Commission expert reviewer in the field of mobile commerce. Described in *The Independent* in 2004 as a "grade-A geek", he has written for publications ranging from *The Guardian* to the *Parliamentary IT Review* and is a media commentator on electronic business issues.

This draft 13/9/05, 4620 words (9 pages)

An edited version of this article appeared in *Prospect* magazine (March 2005).

INFORMATION RETRIEVAL

We are going to have a national identity card scheme. The government's bill won its second reading before Christmas by 385 votes to 92. So it is time to stop talking about whether its a good or a bad thing, whether its a waste of money or whether it will do anything about crime, terrorism, illegal immigration and so on. Instead, we should focus on how to make the scheme work well for all stakeholders. For that we need some knowledge of what technology can and cannot do.

Let's be clear. So far as privacy is concerned, in a society where huge databases—private and public—store information about many aspects of a citizens life, identity cards are a privacy sideshow. We must not concentrate on the cards in isolation. When he was home secretary, David Blunkett hypothesised that if you could develop cheap and effecitve biometrics—the use of unique physical identifiers—then a card would be superfluous. If you decided to go swimming at the leisure centre, you would stroll in, a machine would scan some relevant physical detail (a CCTV camera looking at your face, to give the obvious implementation), look you up in the government database, pass your details to the local authority (to charge the fee to your account) and to the police (to check you're not on an offenders' register or whatever). There's no need for a card in that world, but I think that version of the future is wrong and that a card is desirable. But to see why, we need to look at what the identity scheme should do and how it might do it.

separating the card from the register

The scheme proposed by the British government has two components: a national identity register and a national identity card. The register is used to assign everyone in the country a unique identifier: let's call it the citizen number. (Everyone here means people with citizenship, a right to remain or a leave to stay in Britain.) Two lots of computers are needed to implement this scheme. One lot of computers will form the register in a government building somewhere. Their focus will be preventative, stopping people from doing things that they want to do such as claiming benefits that they are not entitled to or working illegally. Another lot of computers (the government hopes) will be built into smart identity cards in people's pockets. Their focus should be on enabling people to do things that they want to do: such as opening bank accounts and getting served in pubs.

Now, a great many of the governments goal's—especially relating to the delivery of public services—could be met simply by building the register and then stopping. The efficiency of service delivery in welfare benefits, health, education and many other areas would be improved if everyone had a unique number that was easily verifiable as belonging to them. Goodness knows how much money is wasted because a council might have dozens of databases and be unable to establish whether John Smith on one database is that same John Smith on another database.

So let's take it as read that some form of register is a good idea. Incidentally, it's a difficult enough job by itself: in October the head of the e-government unit, Ian Whatmore, told the BBC that a national identity register shared by government agencies is technologically impossible. Since it is in fact technologically possible, what I'm sure he meant was that it is impossible to build such a register, share the information between agencies and keep it secure, which is a slightly different issue.

Security is, naturally, central to the planning of the infrastructure. To achieve it, the register will associate some biometric identifiers (fingerprint, iris pattern and facial image, for example) with each citizen number in order to ensure that each of the numbers is linked to a unique individual and to stop people from obtaining more than one number. (Biometrics are neither as good as their proponents contend nor as bad as their critics allege. Some of the biometrics work pretty well, but no one method is good enough, which is why the scheme will need more than one biometric. And that it turn means recording multiple biometrics for all your citizens—a complex and costly business. But some experience of biometric capture is currently being acquired in the UK passport services trial enrollment of 10,000 people.)

The register, not the card, is where worries about privacy should be focussed. It is quite proper to be concerned about the future misuse of a register, whatever the intentions of those setting it up. A few months ago a DVLA employee was sentenced to five months in prison for using DVLA computers to look up addresses associated with certain car registration numbers and passing them on to animal rights terrorists (as a result of which a number of homes were attacked). This kind of abuse could be replicated on a grand scale in the proposed register.

In security terms, it makes sense to assume that data returned by the register is not confidential and therefore should be kept to a bare minimum. The government's ID card bill suggests, as an example, that national issurance numbers (NINos) should be stored on the register. There is already a database of NINos so it's hard to see why we need another one. I can see that it would be very useful for the NINo database to store each citizens' unique number (to detect stolen and duplicated NINos) but I can't see why it would be useful for the register to store NINos. Storing that kind of data would run the risk of turning the register into a one-stop-shop for identity thieves. Similarly, the national police computer or the DVLA computer or NHS health records could have the unique citizens numbers alongside names without any of the information in those computers being available on the central register.

In fact, it is not obvious why the register should contain names, addresses or any other personal information at all. If the purpose of the register is to ensure the unique and verifiable correlation between a citizens number and a citizens biometric, then it need contain nothing other than those two things. This is how EURODAC, the EU fingerprint database for asylum seekers, works: it only holds the biometric templates and no other information and the only query that law enforcement officials can make is "is this fingerprint in your database or not?" (Since it started operation in 2003, the system has detected that 7 per cent of asylum applications are apparently repeats.)

As any security expert will tell you, complexity is an enemy. It will be a difficult enough job to build the security that we should all expect of the register (keeping our biometric data confidential) without adding more information and more transactions (such as change of address) that need to be secured. We should resist this kind of function creep for all of the reasons identified by both civil rights commentators and security experts: we don't know what some future parliament might decide to do with the register might. Let's keep the register simple, viable and limited in scope. Then let's build a smart ID card to work with it.

a smart id card for the 21st Century

The 21st-century ID card that we should aim for has nothing in common with the 20th-century card that Britain had from 1939 to 1952. That was just a piece of cardboard and used no modern technology other than printing. The 21st century card will, by contrast, depend on three key technologies: microcomputers, biometrics and digital signatures.

To work out how to use these technologies to make modern ID cards, we need to reflect a little more on what such a card might be used for. The idea of ID cards in the abstract is popular but as the costs and drawbacks become clearer support may start to slip. This programme is going to cost billions of pounds and voters are going to find themselves being charged real money to get an ID. And the first pensioner to get fined £2,500 because they forgot to register a change of address will become a cause celebre. A card that is just a badge of citizenship but does nothing for people except cause hassle will never sustain support. The card has to provide a special service for citizens that they can't get without it. Somewhat counter-intuitively, that special service may well be privacy.

The glory of using computers, biometrics and digital signatures is that they can work together to disclose facts about someone without disclosing their full identity. Your ID card could, for example, send a message to a machine confirming that you are over 18 without disclosing who you are or what your citizen number is. The receipient of that message—Ladbrokes, say—would know that the digital signature from the ID card is real and that the message had not been forged and let you place a bet: but who you are could remain confidential. To understand how, you have to know a little about the technologies mentioned above.

Microcomputers first. ID cards will have computers on them. Just like those chip and PIN credit and debit cards, the cards will contain tiny, tamper-resistant computers. This is a very important point. People can't see what's held securely in the computers. Therefore, the only way that a hospital receptionist will be able to tell whether a patients card is valid or not is by using a machine to check that the biometric corresponds with the person. Anything that is printed on a card could be forged or altered, so whatever is printed on an ID card face is largely irrelevant. We should probably restrict the front of the card to a simple picture of the holder and the citizen number. (Putting names and other details on the front of cards means that they will inevitably be stolen to commit identity fraud but if there's no identity on the front, there's nothing to steal.)

What's inside the computer on the ID card is critical. The receptionist's machine could work in one of two ways, depending on the architecture of the scheme. Let's assume that fingerprint is the biometric. The machine could either obtain the citizen number from the card and then send the number, plus the fingerprint, off to the register for checking (what IT people call a centralised system) or the machine could give the fingerprint to the card and ask the card (since the card has a computer in it, remember, the could store its owner's biometrics) whether the fingerprint is that of its rightful owner (just as the new "chip and PIN" credit cards check the PIN you type in by themselves and then tell the retailer's till whether the PIN was correct or not). In the latter case (what IT people call a distributed system) the register will be spared millions of queries every day.

The government is undecided about whether to store biometric templates in the cards. It ought to. Firstly because other related initiatives have gone in this direction (including the International Civil Aviation Authority, ICAO, standard for smart passports which stores a biometric—your facial image—in the computer chip inside the passport) and secondly because almost all of the day-to-day usage of the card could work this way, thus significantly reducing the cost and complexity of the register. Imagine how many computers will be need if the register has to manage all these queries! And what would happen if the network broke down, or the computers went wrong? If the receptionist's machine can work "stand alone", the overall system is much more resilient and reliable.

The final piece of the technological jigsaw is the digital signature. Understanding digital signatures requires a great deal of knowledge of mathematics and cryptography. Suffice to note here that if you attach a digital signature to some information (an email message for example) then it means two things: first, if anyone changes the information then the signature will no longer be valid (so that you can detect tampering); and second, you know who the information came from (this is because the signature depends on a security key as well as the information, so if you know who the key belongs to then you know who made the signature).

But how do you know who the key belongs to? That's the clever bit. Digital signatures use something called "public key cryptography". A person (or an organisation) has two mathematically-related keys. These are the private key and the (hence the name) public key. In the context being discussed here, the private key would live inside your ID card. The public key would be know to, well, the public. If you want to send your bank a signed message, you sign it using your private key. Your bank knows your public key, so they can check the signature. A potential fraudster could not use your public key to guess your private because of the mathematics linking the two: it's all to do with large prime numbers and so intractable that legions of supercomputers would take millions of years... you know the score.

now let's put all the technologies together in an ID card.

Your ID card would contain your private key and only you would be able to use it. The card won't sign anything unless it is given your fingerprint or PIN. Your identity, in a very real sense, then becomes your public key. That wouldn't be much use to the council or the pub (or anyone else: how would they know that it's your public key and not someone else's), so the public key is stored inside a digital certificate that contains, for example, some identifier (eg, an e-mail address) together with some credentials (eg, is over 18) cryptographically secured by someone else (eg, the Home Office). Now, the council doesn't have to trust me, because I present them not with a key (which is just a string of bits) but with a certificate digitally-signed by the Home Office.

In principle anyone can issue such certificates. My bank could issue a digital certificate to my kids, perhaps. This way, my 10 year old could go into his Halo chat room (Halo is a computer game, m'lud, beloved of 10 year old boys) as "UK_terminator@cooldomain.com" or whatever, but not be able to gain access to a chat room for over 18s. This isn't a way of hiding from anyone or getting up to no good. If I get up to no good in a chat room as Donald Duck, then the police will simply take a warrant to my bank who will tell them precisely who Donald Duck is.

I would argue that we could use these identity technologies to develop a much more flexible and sophisticated national identity infrastructure than may at first be apparent. For one thing, the technologies discussed here mean that people can have lots of "virtual identities" if they want: your public key might be in all sorts of different certificates signed by different people for different reasons and your ID card might be allowed to generate its own private keys for you to use in different environments. This is a very good thing. I don't want my kids using their real names in Internet chat rooms any more than I want hospital whistleblowers to have use their real names: a nurse, for example, ought to be able to send an e-mail (to report lax hygeine routines, perhaps) with a digital certificate that proves that she is a nurse but not who she is.

The advantage of this approach lays in the relationship between mathematics and economics. If it is technically possible to find out who has done what—when a crime has been comitted, for example—but it is economically prohibitive (because of cryptography) to monitor people continuously on a large scale, then a reasonable "privacy settlement" can be achieved.

id cards can increase privacy

Consider an example where using an ID card ought to improve life: starting a new job. A person goes along goes to the office on the first day and produces his card. The employer has no way of knowing whether the card is valid, so they will have to use a PC to read it. The PC can check whether the card is real (from its digital signature) and display the picture held inside the computer chip so that the employer can see that it's the right person. The employer submits the citizen number to the Inland Revenue when required and the Inland Revenue can quickly match the individual with the correct taxpayer record (without the employer having access to any confidential tax information about the new employee) and generate a PAYE code for the accounts department. This process saves the employer and the employee time and effort (and cuts out errors).

Take another simple case: getting a drink. In a few years time, when you walk into a nightclub you may have to wave your card over a reader by the door: the reader displays a red cross if you are under 18 or the picture from inside the chip if you are over 18. The doorman can see whether the picture displayed is you or not and so decide whether to let you in or not: the barman will not, however, know who you are.

It is because of these privacy issues that I think that Blunkett was wrong to say that cards may become irrelevant. In the overwhelming majority of cases where someone will be using their card, it will not be to prove who they are, but rather to prove something about themselves: they are entitled to be in Britain, are over 18 or allowed to read a particular e-mail. A properly designed ID card can disclose such credentials with no need for access to the register or unwarranted disclosure of identity.

It isn't all about credentials, of course. There are some cases where citizens will use the ID card to prove who they are. Opening a bank account, for example. One could envisage being able to open a new account by wandering up to a cash machine in a bank branch, putting your eye up to the camera and waving your ID card around: no forms, not gas bills, no passports, photocopies of driving licences and so on. ID cards would save citizens time and banks money.

identity in cyberspace

The examples of chat rooms, the Internet, and e-mail lead us to the place where a privacy-enhancing identity service is most desperately needed: cyberspace. If the government is wise enough to build an ID card that works online as well as offline, they might not only cut fraud and crime but stimulate the new economy in important ways. If ID cards were to contain the software for making digital signatures then it means that when you logged on to your bank, the Inland Revenue or Tesco, then they could be certain that it was you and you could be certain that they are who they say they are and not Ukrainian fraudsters (because your ID card and the bank's computer would be able to check each other's digital certificates).

This may sound complex, but it's actually not that difficult to implement because almost all of the web browers and web servers in the world already contain the standard software to do this. They just don't use it because it's a big problem for them to give every consumer a secure virtual identity. If the government did this for them, then they would all use it and online fraud (such as the hundreds of millions lost to "card not present" payment card fraud in the UK last year) should fall.

Hong Kong has one of the smartest smart ID cards in the world and it uses digital certificates to give citizens just that kind of security online. Citizens who want to use their ID card on the web go to Hongkong Post and buy a digital certificate which is downloaded to their card. They can then, for example, log in to online shopping sites in complete security. Why can't we do the same? Online banking, online shopping and (hopefully one day) online government would be transformed by an ID card that worked this way. Furthermore, if ID cards had digital signature software in their computers, then you could send emails to your bank, your employer or your MP and they could be certain that the emails came from you and not a fraudster or other undesirable. This is where they are going in Estonia, where their smart ID card uses internationally-standardised digital signature software. You sit down at your computer and put your card in the reader (a simple USB smart card reader is about a fiver) and punch in your PIN and off you go. No one can pretend to be you in an email and no-one can read your email even if they steal your computer: your could have your mail remain encrypted in your inbox: without your ID card, the mail is just random numbers to a thief.

Despite the fact that neither digital signatures nor digital certificates are mentioned in the current bill, I'm sure that the government will want to do something in this area because it would make a real difference to the average British internet user. It really isn't that complicated (in fact, its easier doing this with ID cards than without them because your ID card would carry your keys and digital certificates everywhere).

Digital signatures have been around for years and there are all sorts of standards for storing and transmitting the certificates and the keys. Industry is perfectly capable of coming up with ways of building them into products (in Belgium, Microsoft has announced that it will integrate the Belgian national smart identity card into its MSN software for chatrooms and so on) and there are a great many business old and new that would take advantage of the infrastructure. Imagine how much simpler life would be for eBay if you could log on with your ID card (which eBay would trust because it knows the Home Office's public key) and generate an eBay identity that all the marketplace participants could trust.

identity management that works

Building a useful national identity management scheme is a huge undertaking that needs to balance many interests without becoming a tangled mess. As the government develops a more technologically-informed vision of the scheme it ought to look rather different from the current vision set out in the bill. In particular, the idea that the register should store all personal details needs to be abandoned as soon as possible. If the register is restricted to storing citizen numbers, biometric templates and digital certificates only, then the cost and complexity of registering people falls because you wouldn't need to collect all different kinds of data from them. And you wouldn't have to fine them £2,500 for forgetting to register a change of address, because the register wouldn't have their address on it.

If the ID card is made smart enough to verify biometric templates and use digital signatures to disclose credentials without identity then its usefulness is significantly enhanced and, since it would then protect individual privacy, so is its attractiveness. Looking at an ID card this way—as a fundamental enabler of services and a means for individuals to take control of their information identities and enhance privacy—is a very different and far more optimistic perspective than that defined by the current "electronic cardboard" vision.

If we're going ahead, let's have a scheme that works and lets be realistic about what it can do. And let's be clear. No card is a magic bullet against crime and terrorism by itself. If you're a policeman trying to find out whether Dave Birch is really Joe Bloggs then it's the register that will tell you. If you're a local council trying to find out if Dave Birch is already claiming housing benefit under another name, it is the register that will help you (since all housing benefit databases will be updated to store the citizen number of claimants).

From a privacy perspective, an national ID card makes no difference. But I want one, because a card that used modern technology effectively would be better for all of us than either a giant database or no card at all. So let's make the register cheaper and simpler (and have some hope of it actually being built and working properly) and then let's set about developing a card that will make life better.

This isn't just yet another huge government IT project. It's a unique piece of infrastructure for a modern society. Implemented badly, it will make our lives (and our tax bills) immeasurably worse. Implemented well, it could make them substantially better. It's important to care.

REFERENCES

1. Raines, R. *Identity Cards* in proc. of *International Association for Biometrics*, iAfB (London: Sep. 2004)

2. Blunkett, D. *Identity Card Speech* in *IPPR.* (18th Nov. 2004).

3. Wakefield, J. *Whitehall shifts digital priorities* in *BBC News Online.* (18th Oct. 2004).

4. Beckley, A. *The future of privacy in law enforcement: the United Kingdom's experience* in *The FBI Law Enforcement Bulletin.* (1st Sept. 2004).

5. *DVLA man helped animal activists* in *BBC News (UK Edition).* (25th Oct. 2004).

6. Olsen, F. *E-signatures navigate troubled waters* in *Federal Computer Week.* (31st May 2004).

7. *European database reveals 7 percent of asylum seekers apply in more than one country* in *AP Worldstream.* (5th May 2004).

8. Singh, S. *Pretty Good Privacy* in *The Code Book*. p. 293-316, Fourth Estate (London: 2000).

9. *Great taste, less privacy* in *Wired News.* (6th Feb. 2004).

10. Birch, D., *Identity cards and financial services: how will the introduction of ID cards affect financial services providers?* Journal of Internet Banking and Commerce, 2005. **9**(3).

11. Castells, M. *Privacy and Liberty in Cyberspace* in *The Internet Galaxy*. p. 168-187, OUP (Oxford: 2002).

12. Birch, D. *Who Are You? A simple question with many answers* in proc. of *Security and Privacy*, Vanguard (Austin: Feb. 2004)

13. *Fighting the worms of mass destruction* in *The Economist.* **369**(8352): p. 101-103 (29th Nov. 2003).

14. Birch, D. *So you know who I am?* in *Public Servant.* (10): p. 18 (10th Sep. 2004).

15. *New Internet shopping hot spot at ShopThruPost* in *e-Cert Newsletter.* (12) (Dec. 2004).

16. Martens, T. *The Estonian National Identity Card* in proc. of *Digital Identity Forum*, Consult Hyperion (London: Nov. 2004)

consult hyperion
www.chyp.com

Dave Birch

Digitally signed by Dave Birch
DN: cn=Dave Birch, c=GB, l=Guildford, st=Surrey, o=Consult Hyperion, ou=Private Website, email=dave.birch@chyp.com
Reason: I am the author of this document
Date: 2005.09.13 14:40:01 +01'00'